Дополнение для любознательных: работа с DNS-записями

Это сплошная теория, её можно не читать, задания тут нет. Прочитайте этот урок, если хотите лучше понять, как работают DNS-записи, которые вы настроили в прошлом уроке.

Мы с вами настроили 3 записи. Их настройка снижает вероятность попадания письма в спам: при любых разборах ситуации, когда письмо оказалось в спаме первым делом стоит проверять именно настройки этих записей. Как они работают? Какая информация в них содержится? Я использовал удачные описания отсюда и отсюда.

🏆 **SPF** — определяет откуда отправлять письма;

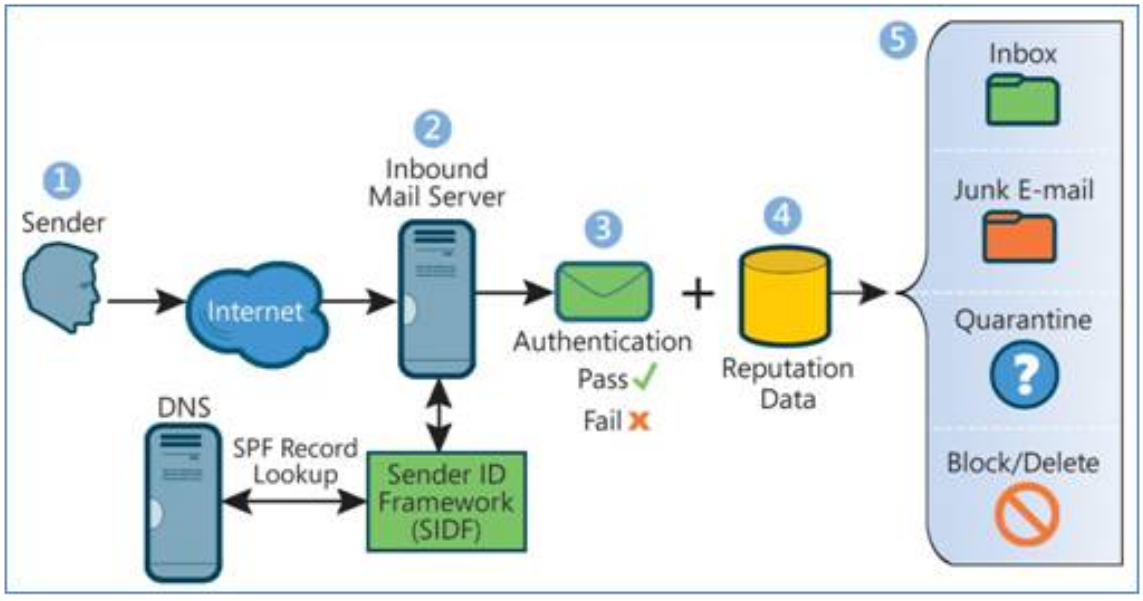
🏆 **DKIM** — подпись для защиты от подделок;

🏆**DMARK** — определяет, что делать с подозрительными письмами, которые отправлены с неправильными spf и/или dkim.

Если бы этих механизмов не было, то любой компьютер в сети мог бы отправлять письма от имени любого домена.

SPF (sender policy framework)

Это подпись, содержащая информацию о серверах, которые могут отправлять почту с вашего домена. Наличие SPF снижает вероятность попадания вашего письма в спам.



- запись типа txt;
- содержит список серверов, которые могут отправлять почту от имени домена (в нашем примере это почта mail.ru и сервис рассылок Unisender);
- может включать одиночные сервера или подсети;
- может импортировать список с другого домена (Это в частности происходит с unisender: мы не знаем все его ip-адреса и в spf даём команду считать его из unisender. Если же нужно просто использовать запись с другого домена, не дополняя её, то лучше всего использовать redirect);
- у домена может быть только одна spf запись (это очень частая ошибка в ДЗ);
- spf не действует на поддомены (у каждого поддомена должна быть своя spf-запись).

Если интересно, то она расшифровывается так:

v=spf1 ip4:00.00.000.00.0 pinclude:spf.unisender.com ~all

«v=spf1» — версия SPF, обязательный параметр, всегда spf1, никакие другие версии не работают;

«+» — принимать письма (по умолчанию);

«-» — отклонить;

«~» — «мягкое» отклонение (письмо будет принято, но будет помечено как спам);

«?» — нейтральное отношение;

«mx» — включает в себя все адреса серверов, указанные в MXзаписях домена;

«ip4» — позволяет указать конкретный IP-адрес или сеть адресов;

«a» — IP-адрес в A-записи;

«include» — включает в себя хосты, разрешенные SPF-записью указанного домена;

«all» — все остальные сервера, не перечисленные в SPF-записи;

«ptr» — проверяет PTR-запись IP-адреса отправителя (разрешено отправлять всем IP-адресам, PTR-запись которых направлена на указанный домен) (не рекомендуется к использованию согласно RFC 7208);

«exists» — выполняется проверка работоспособности доменного имени;

«redirect» — указывает получателю, что нужно проверять SPF запись указанного домена, вместо текущего домена (redirect:spf.example.com).

Так как запись должна быть всего одна, через include необходимо прописывать все возможные сервера, через которые вы отправляете письма.

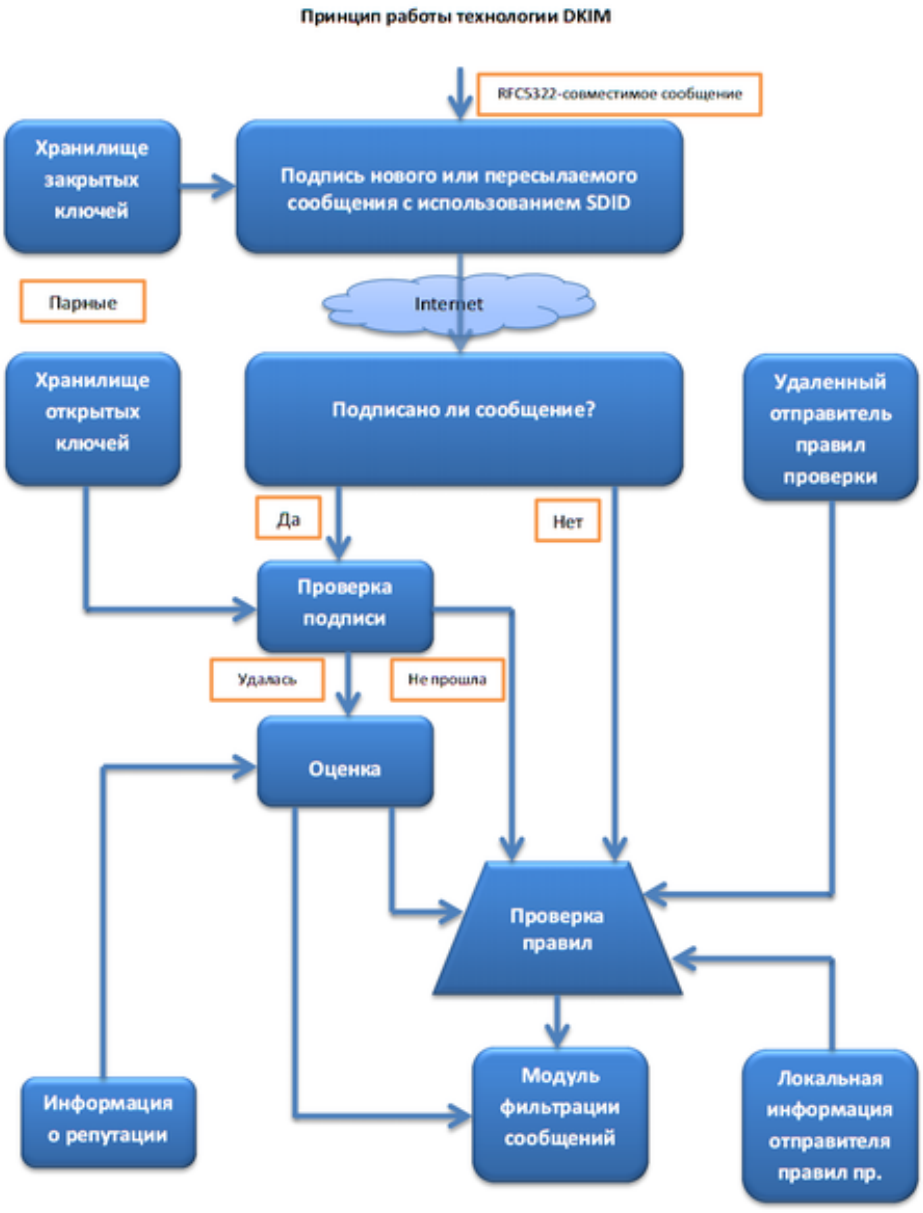
Посмотреть вашу spf можно тут

https://easydmarc.com/tools/spf/

DKIM (Domain Keys Identified Mail)

Это цифровая подпись, которая подтверждает подлинность отправителя и гарантирует целостность доставленного письма. Подпись добавляется в служебные заголовки письма и незаметна для пользователя. DKIM хранит 2 ключа шифрования — открытый и закрытый. С помощью закрытого ключа формируются заголовки для всей исходящей почты, а открытый ключ как раз добавляется в DNS записи в виде TXT файла.

Проверка DKIM происходит автоматически на стороне получателя. Если домен в письме не авторизован для отправки сообщений, то письмо может быть помечено подозрительным или помещено в спам, в зависимости от политики получателя.



Записей DKIM может быть несколько — например, если вы пользуетесь одновременно сервисом Unisender и при этом отправляете письма через biz.mail.ru, у вас будет 2 записи DKIM с разными селекторами.

Обязательные элементы:

«v» — версия DKIM, всегда принимает значение v=DKIM1;

«k» — тип ключа, всегда k=rsa;

«p» — публичный ключ, кодированный в base64.

Необязательные элементы:

«t=y» — режим тестирования. Нужно только для отслеживания результатов;
«t=s» — означает, что запись будет использована только для домена, к которому относится; не рекомендуется, если используются субдомены;
«h» — предпочитаемый hash-алгоритм, может принимать значения «h=sha1» и «h=sha256»;
«s» — тип сервиса, использующего DKIM. Принимает значения «s=email» (электронная почта) и «s=» (все сервисы). По умолчанию «*»;*
«;» — разделитель.

Посмотреть записи для своего домена можно здесь:

https://easydmarc.com/tools/dkim/

DMARC (Domain-based Message Authentication, Reporting and Conformance)

Это подпись, которая позволяет принимающему серверу решить, что делать с письмом. DMARC использует DKIM и SPF. Если отправленное сообщение не прошло проверку DKIM и SPF, то оно не пройдет и DMARC. Если же сообщение успешно прошло хотя бы одну проверку (DKIM или SPF), то и проверку DMARC сообщение пройдет успешно. DMARC добавляется только после того, как настроены записи SPF и DKIM.

Пример записи DMARC (не имеет значения, какими сервисами для рассылки вы пользуетесь):

v=DMARC1; p=reject; sp=reject; ruf=mailto:postmaster@your.tld; fo=1

«v» — версия, всегда принимает значение «v=DMARC1» (обязательный параметр);
«p» — правило для домена (обязательный параметр). Может принимать значения «none», «quarantine» и «reject», где «p=none» не делает ничего, кроме подготовки отчетов; «p=quarantine» добавляет письмо в спам; «p=reject» отклоняет письмо.
Тег «sp» отвечает за субдомены и может принимать такие же значения, как и «p».
«aspf» и «adkim» позволяют проверять соответствие записям и могут принимать значения «r» и «s», где «r» — «relaxed» (более мягкая проверка), а «s» — «strict» (строгое соответствие).
«pct» отвечает за кол-во писем, подлежащих фильтрации, указывается в процентах, например, «pct=20» будет фильтровать 20% писем.
«rua» — позволяет отправлять ежедневные отчеты на email, пример: «rua=mailto:postmaster@your.tld», также можно указать несколько email через запятую без пробелов.
«ruf» — отчеты для писем, не прошедших проверку DMARC.
Тег «fo» служит для генерации отчетов, если один из механизмов сломается. «fo=0» (используется по умолчанию) — присылать отчет, если не пройден ни один этап аутентификации; «fo=1» — присылать отчет, если не пройден хотя бы один этап аутентификации; «fo=d» — присылать отчет, если не пройдена аутентификация DKIM; «fo=s» — присылать отчет, если не пройдена аутентификация SPF.

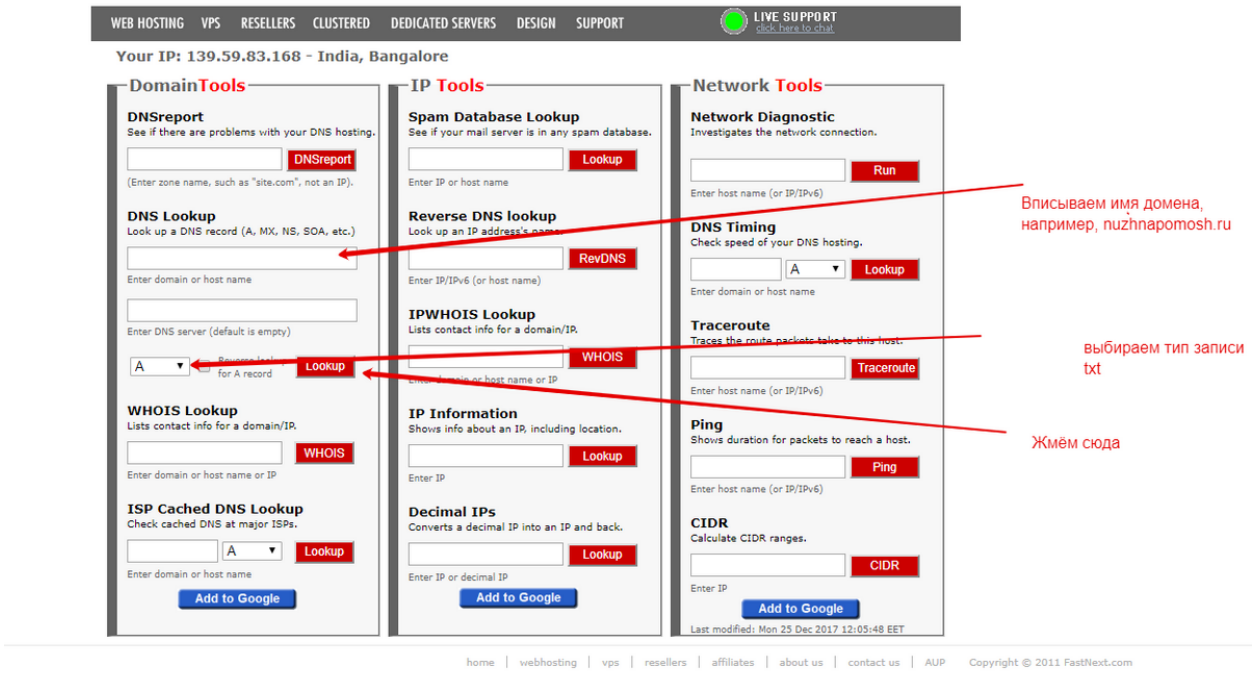
Запись DMARC может быть одна для домена и поддоменов, т.к. в ней можно явно указать действия для тега *«sp»*. Если вам требуется специфическая запись для поддоменов, можно создать отдельную запись с наименованием *«_dmarc.ваш_поддомен.ваш_домен.»*.

Посмотреть запись можно здесь

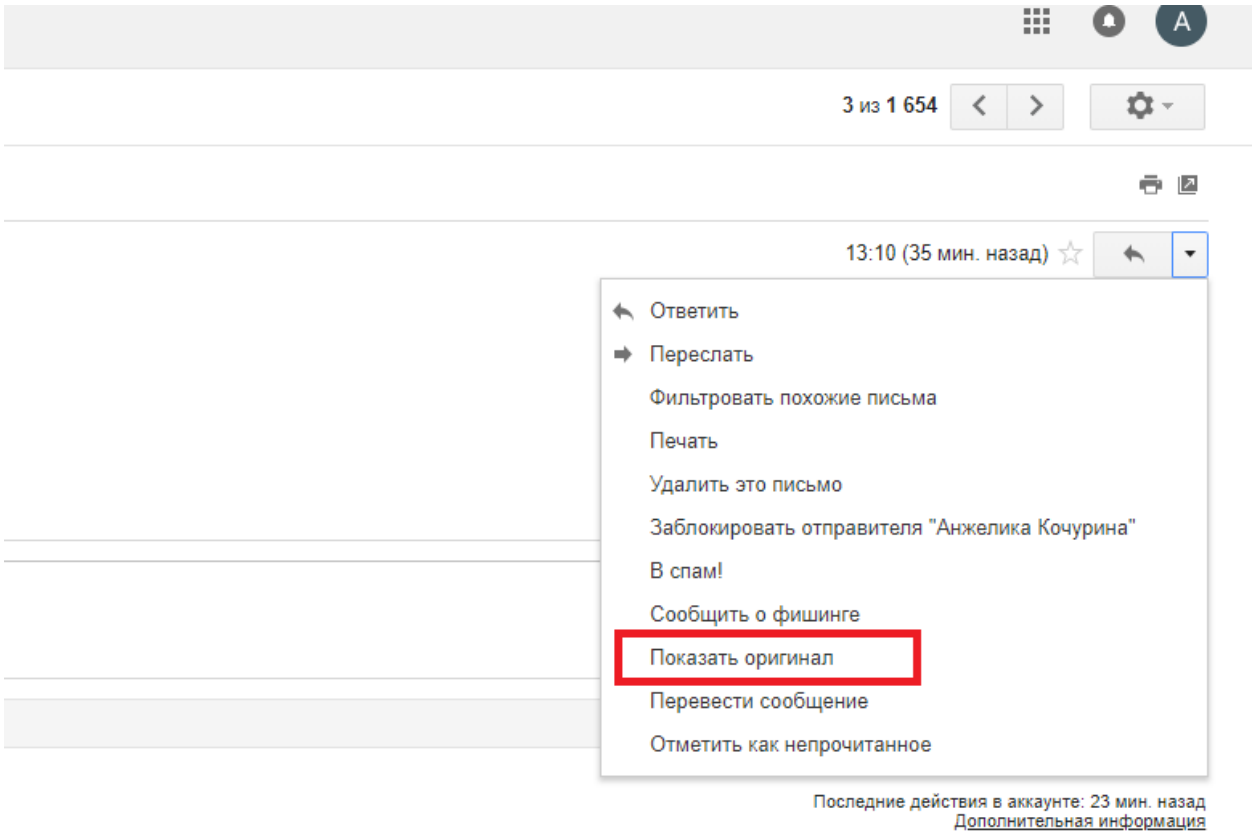
https://easydmarc.com/tools/dmarc/

И немного иллюстраций

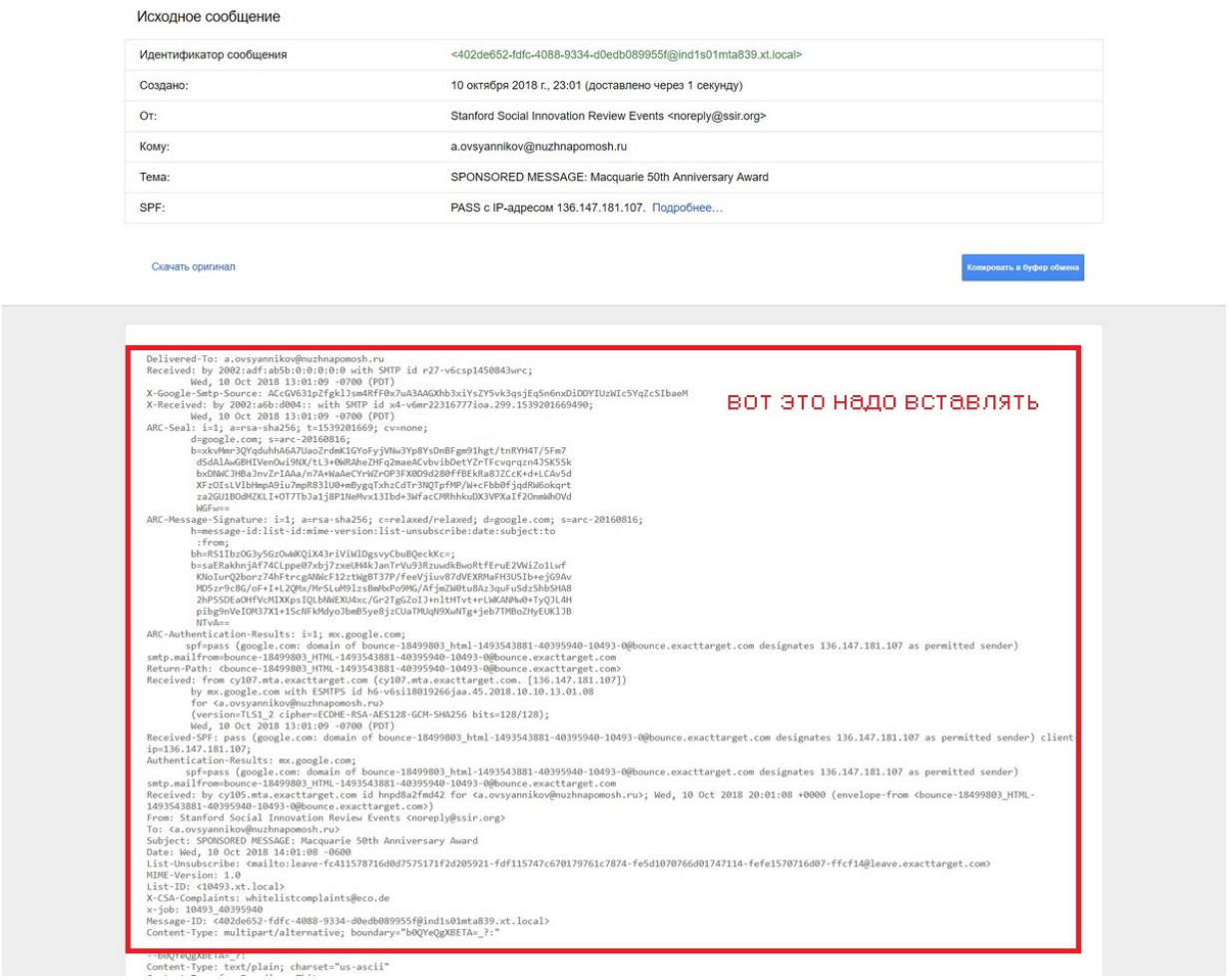
1. Посмотреть, как именно для почтовых серверов выглядят DNS-записи (обновились ли записи, которые вы отредактировали) можно при помощи сервиса http://dnstools.fastnext.com/



2. Если написать письмо себе на любой адрес gmail.com, а потом выбрать в меню опцию "Показать оригинал" можно увидеть письмо целиком, с так называемыми техническими заголовками. Уже на этом этапе вы увидите как прошли проверки.



Вот так это выглядит:



Исходное сообщение

Идентификатор сообщения	<402de652-fdfc-4088-9334-d0edb089955f@ind1s01mta839.xt.local>
Создано:	10 октября 2018 г., 23:01 (доставлено через 1 секунду)
От:	Stanford Social Innovation Review Events <noreply@ssir.org>
Кому:	a.ovsyannikov@nuzhnapomosh.ru
Тема:	SPONSORED MESSAGE: Macquarie 50th Anniversary Award
SPF:	PASS с IP-адресом 136.147.181.107. Подробнее...

Скачать оригинал

Копировать в буфер обмена

ВОТ ЭТО НАДО ВСТАВЛЯТЬ


```
Delivered-To: a.ovsyannikov@nuzhnapomosh.ru
Received: by 2002:adf:ab5b:0:0:0:0:0 with SMTP id r27-v6csp1450843wrc;
        Wed, 10 Oct 2018 13:01:09 -0700 (PDT)
X-Google-Smtp-Source: ACcGV631pZfgklJsm4RfF0x7uA3AAGXhb3xiYsZY5vk3qsjEq5n6nxDiDDYIUzWIc5YqZcSIbaeM
X-Received: by 2002:a6b:d004:: with SMTP id x4-v6mr22316777ioa.299.1539201669490;
        Wed, 10 Oct 2018 13:01:09 -0700 (PDT)
ARC-Seal: i=1; a=rsa-sha256; t=1539201669; cv=none;
        d=google.com; s=arc-20160816;
        b=xkvMmr3QYqduhhA6A7UaoZrdmK1GYoFyjVNw3Yp8YsDnBFgm91hgt/tnRYH4T/5Fm7
         dSdAlAwGBHIVenOwi9NX/tL3+0WRAheZHFq2maeACvbvibDetYZrTFcvqrqzn4JSK5Sk
         bxDNWCJHBaJnvZrIAAa/n7A+WaAeCYrWZrOP3FX0D9d280ffBEkRa8JZCcK+d+LCAv5d
         XFzOIsLVlbHmpA9iu7mpR83lU0+mBygqTxhzCdTr3NQTpfMP/W+cFbb0fjqdRW6okqrt
         za2GU1BOdMZKLI+OT7TbJaij8P1NeMvx13Ibd+3WfacCMRhhkuDX3VPXaIf2OnmWhOVd
         WGFw==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816;
        h=message-id:list-id:mime-version:list-unsubscribe:date:subject:to
         :from;
        bh=RS1IbzOG3y5GzOvWKQiX43riViWlDgsvyCbuBQeckKc=;
        b=saERakhnjAf74CLppe07xbj7zxeUM4kJanTrVu93RzuwdkBwoRtfEruE2VWiZo1Lwf
         KNoIurQ2borz74hftrcgANWcF12ztWgBT37P/feeVjiuv87dVEXRMaFH3U5Ib+ejG9Av
         MD5zr9c8G/oF+I+L2QMx/MrSLuM9lzsBmMxPo9MG/AfjmZW0tu8Az3quFuSdzShbSHA8
         2hP5SDEaOHfVcMIXKpsIQLbNWEXU4xc/Gr2TgGZoIJ+nltHTvt+rLWKAN9w0+TyQJL4H
         pibg9nVeIOM37X1+1ScNFkMdyoJbmB5ye8jzCUaTMUqN9XwNTg+jeb7TMBoZHyEUKlJB
         NTvA==
ARC-Authentication-Results: i=1; mx.google.com;
       spf=pass (google.com: domain of bounce-18499803_html-1493543881-40395940-10493-0@bounce.exacttarget.com designates 136.147.181.107 as permitted sender)
smtp.mailfrom=bounce-18499803_HTML-1493543881-40395940-10493-0@bounce.exacttarget.com
Return-Path: <bounce-18499803_HTML-1493543881-40395940-10493-0@bounce.exacttarget.com>
Received: from cy107.mta.exacttarget.com (cy107.mta.exacttarget.com. [136.147.181.107])
        by mx.google.com with ESMTPS id h6-v6si18019266jaa.45.2018.10.10.13.01.08
        for <a.ovsyannikov@nuzhnapomosh.ru>
        (version=TLS1_2 cipher=ECDHE-RSA-AES128-GCM-SHA256 bits=128/128);
        Wed, 10 Oct 2018 13:01:09 -0700 (PDT)
Received-SPF: pass (google.com: domain of bounce-18499803_html-1493543881-40395940-10493-0@bounce.exacttarget.com designates 136.147.181.107 as permitted sender) client
ip=136.147.181.107;
Authentication-Results: mx.google.com;
       spf=pass (google.com: domain of bounce-18499803_html-1493543881-40395940-10493-0@bounce.exacttarget.com designates 136.147.181.107 as permitted sender)
smtp.mailfrom=bounce-18499803_HTML-1493543881-40395940-10493-0@bounce.exacttarget.com
Received: by cy105.mta.exacttarget.com id hnpd8a2fmd42 for <a.ovsyannikov@nuzhnapomosh.ru>; Wed, 10 Oct 2018 20:01:08 +0000 (envelope-from <bounce-18499803_HTML-
1493543881-40395940-10493-0@bounce.exacttarget.com>)
From: Stanford Social Innovation Review Events <noreply@ssir.org>
To: <a.ovsyannikov@nuzhnapomosh.ru>
Subject: SPONSORED MESSAGE: Macquarie 50th Anniversary Award
Date: Wed, 10 Oct 2018 14:01:08 -0600
List-Unsubscribe: <mailto:leave-fc4115787716d0d7575171f2d205921-fdf115747c670179761c7874-fe5d1070766d0174114-fefe1570716d07-ffcf14@leave.exacttarget.com>
MIME-Version: 1.0
List-ID: <10493.xt.local>
X-CSA-Complaints: whitelistcomplaints@eco.de
x-job: 10493_40395940
Message-ID: <402de652-fdfc-4088-9334-d0edb089955f@ind1s01mta839.xt.local>
Content-Type: multipart/alternative; boundary="b0QYeQgXBETA=_?:"

--b0QYeQgXBETA=_?:
Content-Type: text/plain; charset="us-ascii"
```


Если затем вставить эту абракадабру в сервис https://toolbox.googleapps.com/apps/messageheader/analyzeheader, то можно увидеть, пройдена ли проверка spf (spf PASS) и DIKIM (DIKIM PASS).

Артем Овсянников

Digital-директор в фонде «Нужна помощь»